

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Christopher J. Toomey, a United States Federal Bureau of Investigation Task Force Officer, being first duly sworn, hereby depose and state as follows:

I. PURPOSE OF AFFIDAVIT

1. I submit this affidavit in support of an application for a warrant to search the following vehicle (hereafter, the “Target Vehicle”):

**Black 2011 BMW 328i
Bearing VIN WBAPK7C53BF195825
with New Hampshire license plate 496 8496**

Based on the information contained herein, there is probable cause to believe that the Target Vehicle, described in Attachment A, contains evidence, fruits, and instrumentalities of the crime of 21 U.S.C. §§ 841 [Possession with the Intent to Distribute Controlled Substances].

II. AGENT BACKGROUND

2. I am a Task Force Officer (“TFO”) with the United States Federal Bureau of Investigation (“FBI”) having served in this capacity since October of 2020. From 2010 to 2020, I served as a law enforcement officer with the Nashua Police Department, Nashua, New Hampshire. Since 2019, I have been assigned to the Nashua Police Departments Narcotics Intelligence Division.

3. In my law enforcement training and experience, I have had an opportunity to search for, seize, and personally observe what I have recognized to be and what was later confirmed by drug analysis to be scheduled drugs, including but not limited to heroin, fentanyl, methamphetamine, cocaine, marijuana (both dried and growing), crack cocaine, and various

narcotics lawfully available only by prescription. I have conducted or participated in among other things, surveillance, undercover transactions, debriefings of informants and confidential human sources, and reviews of taped conversations relating to narcotics trafficking. I have assisted in many other investigations, both state and federal. I have drafted drug related search and arrest warrants and have assisted in the execution of numerous search and arrest warrants in which controlled substances, drug paraphernalia, drug related electronic data, and other contraband were found. Through my training and experience, I have become familiar with the habits, methods, routines, practices, and procedures commonly employed by persons engaged in the trafficking of illegal drugs.

4. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I also am a “federal law enforcement officer” within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

5. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, information received from other law enforcement officers, including their direct examination of relevant documents, and physical surveillance conducted in connection with persons and places mentioned in this affidavit. The purpose of this affidavit is limited to showing that probable cause exists to support the issuance of an arrest warrant and criminal complaint. Accordingly, while this affidavit contains all the material information, I am aware of that is pertinent to the requested arrest warrant and complaint, it does not include each and every fact known by me or other investigators concerning

the investigation.

III. STATUTORY AUTHORITY

6. This investigation relates to an offense committed in the District of New Hampshire, to wit: Possession with Intent to Distribute Controlled Substances, in violation of 21 U.S.C. § 841(a)(1). Title 21, United States Code, Section 841(a)(1) makes it a crime for any person knowingly or intentionally to possess with intent to distribute a controlled substance.

IV. PROBABLE CAUSE

7. On July 21, 2021, at approximately 4:35 PM, Officer Fitzpatrick and Officer Collins were assigned to the Nashua Police Department's Problem Oriented Policing (POP) Unit patrolling around Factory Street and Water Street in Nashua. There, they observed a black 2011 BMW 328 bearing New Hampshire temporary registration 291 5326 traveling south on Factory Street. As the vehicle passed the cruiser, the officers noticed that the male operator was manipulating his cell phone. Based on the traffic violation, the officers conducted a motor vehicle stop.

8. Officer Collins approached the driver side window of the vehicle where she recognized the operator and sole occupant as Matthew ESPERSEN from previous police investigations. When she asked for his driver's license, ESPERSEN stated he did not have it with him and verbally identified himself as "Mark Espersen" with an birth date. Officer Collins utilized her Nashua Police cruiser Mobil Data Transmitter and confirmed that ESPERSEN had provided her with a false name and date of birth.

9. Officer Collins asked ESPERSEN to exit the vehicle to speak with her further. He complied. Prior to ESPERSEN exiting the vehicle, Officer Fitzpatrick observed what appeared to be a knife near ESPERSEN's right front pocket. Upon exiting the vehicle, Officer

Collins conducted a pat frisk on ESPERSEN for weapons and removed a pocketknife from his right side. Officer Collins then asked ESPERSEN about his identity. ESPERSEN again provided false information concerning his identity. When confronted, ESPERSEN finally admitted that he had lied about his name and date of birth because his New Hampshire Driver's License was currently suspended. Officer Collins confirmed through the Nashua Police Department that ESPERSEN's driver's license was currently suspended and that he had a previous conviction out of the 9th Circuit Nashua District Court on July 20, 2017 for Operating after Certified as a Habitual Offender. Due to providing a false name and operating with a suspended license, Officer Collins arrested ESPERSEN.

10. During a search incident to arrest, an officer located a small taser like device and \$770.00 US currency in a fanny pack worn around ESPERSEN's chest. A black colored LG cell phone was also recovered from ESPERSEN's persons. While ESPERSEN was being transported to the Nashua Police Department, Officer Fitzpatrick and Officer Collins conducted an inventory of ESPERSEN's vehicle for valuables prior to towing. During the vehicle inventory, they found a blue North Face backpack in the trunk, which held a black Vaultz lockbox and a bb-gun resembling a real firearm. Officer Collins located a key on ESPERSEN's vehicle keychain for the lockbox. Consistent with Nashua Police Department Standard Operating Procedure, Officer Collins opened the lockbox to account for any valuable property contained within it. Upon opening the lockbox, Officer Collins immediately recognized multiple bags containing suspected quantities of controlled substances, including suspected methamphetamine and heroin/fentanyl.

11. Officer Collins stopped the search and took custody of the lockbox, the backpack, and the suspected drugs. The suspected methamphetamine field tested positive for

methamphetamine via TacticID. Based on the officers' training and experience, they believed that several baggies contained heroin/fentanyl due to the packaging (some "fingers of compressed powder), color and characteristics of the powder. These items were seized and sent to the New Hampshire Forensic Laboratory for analysis. In addition to the suspected controlled substances, the lockbox also contained unused glassine bags with blue marijuana leaf imprints, cigar style wrapping papers, and a digital scale commonly used by drug distributors to weigh their product prior to packaging and selling.

12. Given the totality of the circumstances, including the weight of the suspected drugs inside the lockbox, the packaging materials, and the lockbox key located on ESPERSEN's keychain, ESPERSEN was charged with four counts of Possession of a Controlled Drug with Intent to Distribute; a violation level charge for Possession of Marijuana - quantity less than $\frac{3}{4}$ ounce; Disobeying an Officer; and Driving after Suspension.

13. Prior to a post arrest interview with Officer Fitzpatrick and Officer Collins, ESPERSEN waived his Miranda Rights. During the interview, ESPERSEN admitted to providing false identification during the motor vehicle stop and to operating under suspension. ESPERSEN claimed ownership of the vehicle and said he obtained the vehicle the day prior to his arrest. ESPERSEN further stated that he had been the only person to travel in the vehicle, and that no one else had access to his keys or the vehicle. ESPERSEN explained that he locks his personal items because he has a lot of roommates and does not trust them. When confronted about the backpack and lockbox, ESPERSEN denied any knowledge of the items being in his vehicle.

14. On August 18, 2021, Officer Collins obtained search warrants for the black

colored LG cell phone recovered from ESPERSEN's person, as well as the blue North Face backpack that was recovered from the trunk of ESPERSEN's 2011 black BMW. On August 26, 2021, Officer Collins searched the blue North Face backpack and located a second blue colored Samsung cell phone. On September 13, 2021, Officer Collins obtained a search warrant for the blue colored Samsung cell phone.

15. On September 21, 2021, Officer Collins reviewed the results of the forensic phone examinations on the black colored LG cell phone and blue colored Samsung cell phone that were recovered from ESPERSEN's person and backpack. Officer Collins observed text messages between ESPERSEN and multiple unknown subjects. Based on her training and experience, she believes the text exchanges are consistent with ESPERSEN selling heroin/fentanyl and methamphetamine to the unknown subjects.

16. On November 11, 2021, I reviewed the results of the search warrant conducted on the black colored LG cell phone that was recovered from ESPERSEN's person on the day of his arrest on July 21, 2021. I observed several text message conversations between ESPERSEN and multiple unknown subjects which were consistent with ESPERSEN selling heroin/fentanyl and methamphetamine to the unknown subjects. I also observed several pictures of a black BMW believed to be the same black BMW ESPERSEN was stopped in prior to his arrest on July 21, 2021. During a text conversation with a subject listed as "Jay," ESPERSEN explained that he purchased the black BMW with proceeds from ESPERSEN's controlled drug distribution activities. I also observed on the black colored LG cell phone several "selfie" pictures and "selfie" videos of a male subject who I recognized, based on prior drug investigations, as ESPERSEN.

17. On September 2, 2021, the New Hampshire Forensic Laboratory reported that the suspected substances seized from ESPERSEN's vehicle tested positive for, among other controlled substances, 12.36 grams of methamphetamine and 49.2 grams of fentanyl.

18. On November 16, 2021, the Honorable United States Magistrate Judge Andrea K. Johnstone reviewed and signed a federal arrest warrant for ESPERSEN charging ESPERSEN with two counts of possession of schedule II controlled substances with the intent to distribute placing the arrest warrant in an active status.

19. On November 22, 2021, members of the FBI NHSSGTF observed a black 2011 BMW 328i bearing New Hampshire registration 496 8496 (the "Target Vehicle") arrive at Nashua, New Hampshire. One person occupied the Target Vehicle, which was the operator of said vehicle. Upon arrival of the Target Vehicle, the operator was positively identified as ESPERSEN. Once ESPERSEN was positively identified, members of the Nashua Police Department Special Weapons and Tactics Team responded to the location and placed ESPERSEN in custody. It should be noted ESPERSEN was also wanted on multiple state level arrest warrants for sale of a controlled drug, possession of a controlled drug, disobeying an officer and theft by unauthorized taking. Upon first observation of ESPERSEN in the storage unit, ESPERSEN was observed to be within close proximity to a workbench located within the storage unit. ESPERSEN was then directed by members of the Nashua Police Department Special Weapons and Tactics Team to move closer to the threshold of the opening of the storage unit. As ESPERSEN was being secured in handcuffs, ESPERSEN was located just inside of the threshold of storage unit. Due to the small size of the storage unit, members of the Nashua Police Department Special Weapons and Tactics Team observed, in plain view on top of a workbench located within the storage unit, a powder like substance they believed to be

heroin/fentanyl. Once the scene was secured, I responded to the location of the arrest. While standing outside of the threshold of the storage unit, I observed the same powder like substance believed to be heroin/fentanyl located on top of a workbench within the storage unit. At the time ESPERSEN was placed under arrest, a second male subject who was identified as Nearro Forbes ("FORBES"), date of birth, 984, was in the company of ESPERSEN.

20. Upon making contact with FORBES, members of the FBI NH SSGTF asked FORBES for verbal consent to search FORBES' backpack which was in FORBES' possession at the time of making contact. FORBES freely provided verbal consent to the FBI NH SSGTF to search FORBES' backpack. Upon completion of searching FORBES' backpack, .73 grams of a white colored powdery substance believed to be heroin/fentanyl was recovered from within a black colored eyeglasses case. When questioned about the case and aforementioned substance, FORBES stated he responded to the listed storage unit to meet with ESPERSEN in order to obtain a user quantity of heroin/fentanyl. Upon arrival to the storage unit, FORBES stated ESPERSEN handed him the eyeglass case with the substance believed to heroin/fentanyl inside of it. FORBES also stated he often purchases user level quantities of heroin/fentanyl from ESPERSEN and contacts ESPERSEN via cell phone in order to place his order. FORBES was subsequently placed under arrest by members of the Nashua Police Department Problem Oriented Policing Unit for possession of a controlled drug. During a post arrest interview with members of the Nashua Police Department Problem Oriented Policing Unit, FORBES freely, voluntarily and knowingly waived his Miranda Rights and provided the same information FORBES had provided to the FBI NH SSGTF just prior to his arrest.

21. On November 22, 2021, Honorable United States Magistrate Judge Andrea K. Johnstone reviewed and signed a federal search warrant for the aforementioned storage unit

believed to belong to ESPERSEN located at Nashua, New Hampshire.

Upon completion of searching the listed storage unit, members of the NH FBI SSGTF located and seized a powdery substance believed to be heroin/fentanyl on top of the workbench within the storage unit. The Target Vehicle was also seized and transported, under constant supervision, to a secure garage by at the Nashua Police Department located at 28 Officer James Roche Drive, Nashua, New Hampshire, pending this application for a warrant to search it.

22. With the totality of the circumstances, and facts surrounding this investigation, I believe there is probable cause to believe ESPERSEN utilized the Target Vehicle in order to transport the previously listed controlled substances suspected to be heroin/fentanyl that were located within ESPERSEN's storage unit and found in the possession of FORBES. I also believe from the facts surrounding this investigation, there is probable cause to believe there are more illicit controlled substances within the Target Vehicle. Furthermore, with the totality of the circumstance, and facts surrounding this investigation, I believe there is probable cause to believe ESPERSEN utilized his cell phone in order to negotiate the illicit controlled substance transaction between himself and FORBES. It should be noted a cell phone believed to be ESPERSEN's cell phone was observed in plain view to be attached to the dashboard of the Target Vehicle.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. As described in Attachment B, this application seeks permission to search for records that might be found in the **Target Vehicle**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

25. *Probable cause.* I submit that if a computer or storage medium is found in the **Target Vehicle**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Target Vehicle** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer

or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and

timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-

forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VI. CONCLUSION

29. Based on the foregoing information, I submit that this affidavit supports probable cause for a warrant to search the TARGET VEHICLE, describe in Attachment A and seize the items described in Attachment B. The seizure of these items will aid law enforcement in their investigation of various violations of 21 U.S.C. § 841(a)(1) [Possession with the Intent to Distribute Controlled Substances].

REQUEST FOR SEALING

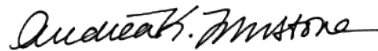
30. I request that the Court order that all papers in support of these applications, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public and/or known to all parties relevant to the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

/s/ Christopher J. Toomey
Christopher J. Toomey, Task Force Officer
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Dec 3, 2021
Time: 5:43 PM, Dec 3, 2021



HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to be Searched

The property to be searched is the entire passenger compartment and trunk or storage space, and any closed or locked containers found therein, including mobile electronic devices, of the

Black 2011 BMW 328i bearing VIN WBAPK7C53BF195825 with New Hampshire license plate 4968496,

which is currently in the possession of the Nashua Police Department at 28 Officer James Roche Drive, Nashua, New Hampshire.

ATTACHMENT B

Description of Information or Items to Be Seized

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 21 U.S.C. § 841 [Possession with the Intent to Distribute Controlled Substances], including information and items related to:

- a. Controlled substances and materials consistent with controlled substances packaging;
- b. Criminal street gang affiliation and criminal street gang activity, such as acts of violence and other criminal activity in furtherance of the criminal street gang or conducted by its members;
- c. United States currency, foreign currencies, and other forms of currency acquired or used during transactions involving contraband;
- d. Places and locations where evidence of the above-referenced criminal offenses was obtained or discarded, or is currently stored;
- e. The identities of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the offenses enumerated in this application;
- f. Electronic devices, including mobile electronic equipment, serial numbers or any electronic identifiers that serve to identify the equipment, and the information stored electronically on the devices, specifically:
 - i. telephone logs, contact lists, other records reflecting names, aliases, addresses, telephone numbers, and other contact or identification data;
 - ii. the actual and attempted possession, purchase, receipt, sale, pawn, trade, transfer, transportation, shipment, or other disposition of controlled substances, including buyer lists, seller lists, notes, pay-owe sheets, records of sales, logs, receipts, and communications;
 - iii. criminal street gang affiliation and criminal street gang activity, such as acts of violence and other criminal activity in furtherance of the criminal street gang or conducted by its members;
 - iv. messages and other communications related to controlled substances and criminal street gang affiliation and activity;
 - v. photographs, images, and depictions of or related to controlled substances violations and criminal street gang affiliation and activity, and currency;

- vi. who used, owned or controlled the equipment;
- vii. when the equipment was used;
- viii. the travel and whereabouts of the user of the equipment;
- ix. the attachment of other hardware or storage media;
- x. the use of counter-forensic programs and associated data that are designed to eliminate data;
- xi. passwords, encryption keys, and other access devices that may be necessary to use the equipment;
- xii. accounts associated with software services or services providing Internet access or remote storage of either data or storage media; and
- xiii. serial numbers and any electronic identifiers that serve to identify the equipment.

II. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. Items described in Paragraph I (a) through (f);
- b. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- d. evidence of the lack of such malicious software;
- e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- f. evidence indicating the computer user’s state of mind as it relates to the crimes under investigation;

- g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- i. evidence of the times the COMPUTER was used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- l. records of or information about Internet Protocol addresses used by the COMPUTER;
- m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" (or "COMPUTER") includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and

other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.